

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT



To:

OKABE Masao

**No. 602, Fuji Bldg.,
2-3, Marunouchi 3-chome,
Chiyoda-ku, Tokyo
1000005 Japan**

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

05. 4. 2005

Applicant's or agent's file reference

10010612WO01

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/JP2005/003253

International filing date (day/month/year)

22. 02. 2005

Priority date (day/month/year)

27. 02. 2004

International Patent Classification (IPC) or both national classification and IPC

Int.Cl. **H04L9/08, H04L9/32**

Applicant

CANON KABUSHIKI KAISHA

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Date of completion of this opinion

17. 03. 2005

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

HIROMASA NAKAZATO

Telephone No. +81-3-3581-1101 Ext. 3597

5M

3365

Form PCT/ISA/237 (cover sheet) (January 2004)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/JP2005/003253

Box No. I Basis of the opinion

1. With regard to the language, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

- ☐ a sequence listing
☐ table(s) related to the sequence listing

b. format of material

- ☐ in written format
☐ in computer readable form

c. time of filing/furnishing

- ☐ contained in the international application as filed.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/JP2005/ 003253

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-18	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

The following document has been considered for the purpose of this report:

D1: JP 11-296327 A (HEWLETT-PACKARD CO.) 1999.10.29

D2: JP 5-327748 A (FUJITSU LTD.) 1993.12.10

D3: JP 2003-308194 A (CANON INC.) 2003.10.31

[Claims 1-4,11,12,15,17]

The subject matter of claims 1-4,11,12,15,17 do not involve an inventive step over D1, D2 and D3 for the following reasons.

D1 discloses a computer which generates a random number, encrypts said random number by a public key, and encrypts print data by said random number as a session key(see paragraph [0043]-[0059], Figs.1-4).

D2 discloses the technical feature of creating a key-encrypting-key data from a password, and encrypting a session key by this key-encrypting-key data(see paragraph [0096]-[0116], fig.15).

D3 discloses a host computer which encrypts the user entered password using a digest algorithm, and transmits this encrypted password to a print server(see paragraph [0011]-[0052], figs.1-8).

The skilled person in the art would easily conceive the idea of employing the key-encrypting-key data created from a password in D2 to substitute the public key disclosed in D1 in order to encrypt the session key, and employing the technical feature of transmitting the encrypted password, which is disclosed in D3.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient,
Continuation of: **V**

[Claims 5-8,13,14,16,18]

The subject matter of claims 5-8,13,14,16,18 do not involve an inventive step over D1 , D2 and D3 for the following reasons.

D1 discloses a printer which receives an encrypted session key and encrypted print data, decrypts said encrypted session key by a secret key, and decrypts said encrypted print data by said session key(see paragraph [0043]-[0059], figs.1-4). And it also discloses that said session key is created at random(see paragraph [0045]).

D2 discloses the technical feature of creating key-encrypting-key data from the user entered password, and decoding an encrypted session key using this key-encrypting-key data(see paragraph [0096]-[0116], fig.15).

D3 discloses a print server which compares the encrypted password contained in a print job with the encrypted password generated inside, and performs printing if both are the same(see paragraph [0011]-[0052], figs.1-8).

The skilled person in the art would easily conceive the idea of employing the key created from the password in D2 to substitute the secret key disclosed in D1 in order to decrypt the encrypted session key, and employing the technical feature of printing data when encrypted passwords are the same, which is disclosed in D3.

[Claims 9,10]

The subject matter of claims 9,10 do not involve an inventive step over D1, D2 and D3 for the same reasons having described above.